Biting the bullet

Engaging your workforce in risk management through an internal communications strategy is an even tougher task when times are hard, explains Graham Buck.

Carmaker BMW's recent announcement of job cuts reinforced a view that companies still keep workers in the dark as long as possible when news is bad – just like the last recession.

But the early '90s were pre-Cadbury and pre-Turnbull, when the concept of good corporate governance was just starting to register. Nearly two decades on, there is much greater awareness of risk management. "An appreciation of the importance of communication, together with the ability to make it happen, are essential competencies for today's risk manager" says Carolyn Williams, development manager at the Institute of Risk Management (IRM).

Hard times having returned, there is a good opportunity to engage employees and emphasise the crucial role they play in ensuring organisations can identify and analyse risks effectively, suggests Jonathon Scott, managing director – change and internal communication at Hill & Knowlton. "The trick is to demystify 'risk management' and put it into language and a context employees understand," he says. "Explaining why it is important is perhaps less of a challenge these days, but workers need to know how they can play a part and not just rely on a 'risk function'."

Too many firms still employ impersonal means of communication such as e-mail, suggests Pan Andreas, head of corporate clients for Towry Law, but open communication is essential

"People see gloomy headlines and their first response is 'What does this mean for me?'" says Andreas. "So companies need a variety of information routes and channels, including newsletters and websites but also offering employees face-to-face sessions.

"At my own firm, the chief executive has been very open about our plans for the coming year, the market conditions we're operating in, how we adapt to them and our future prospects."

A good internal communications strategy also heeds what is being communicated across the range of media, adds Scott. "It's not uncommon for organisations to invest huge amounts to engage employees when this is being undermined by damning press, poor marketing and a damaged reputation. The good news is that this puts risk on employees' agendas – they become keen to find out about it

"Secondly, a good strategy focuses on what is important to employees as well as the company. It's got to be two-way. There's no point in communicating the importance of risk management when employees care more about the lack of car parking spaces. Any move companies make to engage employees without considering this is wasted time."

Scott believes companies shouldn't be afraid to involve employees in risk strategy. "Leaders are often fixated with ensuring that they communicate the exact decisions that have already been agreed at a senior level and are very uncomfortable with communicating ambiguity," he explains.

"This can lead to a sense of 'being done to' by employees and at best achieves complicit agreement. It's much better to have a strategy that outlines what your risk strategy needs to achieve and why. Asking the employees how it can be done helps with emotional engagement, a sense of value beyond the job description and mutual trust."

At insurance and risk management group Aon UK, communications director Charles Willy says the 2009 budget is frozen, but more is being allocated to internal communications

"When brickbats are being hurled, it's easy for leadership to retire behind the office wall. But we follow a strategy based on being out there and visible."

Good communication plays a vital role in risk management.

This includes offering "the most provocative blog in the industry", that of chief executive Peter Harmer. "It's a vehicle that allows people to rant if they wish. Some of the entries can be highly personal, particularly after the pay freeze that we recently announced," explains Willy.

"But times like these teach senior management that people really don't buy 'corporate spin'. Significantly more plain speaking takes place – and we regard that as a good thing."

British companies could also look to Scandinavia for inspiration, adds colleague Alex Hindson, who is also a director of the IRM. "The place where people really 'get' the risk management message is Denmark," he says. "They haven't had the same compliance drivers prevalent in so many other countries. Instead they look at the business values – and if the CEO wants something done, then it gets done."

CRISIS TIPS

What do you do if the worst happens and you are in crisis mode? Sue Copeman talks to Dominic Cockram, managing director, Steelhenge Consulting, who offers the following top tips.

First, open your crisis plan. If you don't have one then follow these tips:

1. Find out what has happened
2. Clearly identify a crisis team and team leader
3. Assess the impact (on your people, assets, customers, reputation)
4. Develop an action plan
5. Develop a timeline of what is happening when
6. Implement the plan
   - How to manage the crisis
   - How to continue your business
   - How to manage your reputation
7. Maintain a log of decisions, actions and issues
8. Develop an internal and external communications plan
9. Look after your staff and their welfare
10. Brief those who need to know on a regular basis
    - Media
    - Staff - upwards and downwards
    - Stakeholders
    - Customers
11. On returning to normality, review how you dealt with what happened and learn the lessons for next time.

Keeping systems up and running

With so many organisations relying heavily upon their IT systems, a sustained period of outage can represent a costly disaster, writes Sue Copeman.

Says Anthony Foy, managing director, Interxion: "The number one thing for businesses in respect of their IT is to have everything up and running in an acceptable way but there are a number of links in the chain. For example, people are looking for very high levels of resiliency in the design of the IT infrastructure, with high service levels and strict penalties."

Some organisations have back-up facilities with specialist providers which they can call on if disaster strikes their inhouse system or premises. For example, Sungard Availability Services provide office recovery suites where employees can relocate should a disaster mean that their normal business location is inaccessible.

These alternative workplaces were widely called upon when floods hit some regions last year. With not only business premises but in some cases homes affected as well, as part of its service Sungard provided some essential personal items as well as the equipment and infrastructure needed to keep the businesses going. Other organisations have taken the route of totally outsourcing their IT facilities. This can be an attractive option financially and there are a number of consultancies like Accenture that provide global IT services. However, it is worth remembering that your business may outsource the IT – but not the IT risk. If something goes wrong, it is your own reputation that will suffer.

In order to prevent problems, Foy suggests that the key points to look for when outsourcing in this way are:

- Availability of power and access to data
- High maintenance standards
- Procedures in place to deal with every kind of incident that can occur within an industrial operating environment
- Good physical security featuring devices such as proximity cards, biometric readers and man-traps (door security)
- Financial security.

PROMOTIONAL FEATURE

Consequence management

"I never thought it would happen to us" and "Someone else will fix it".

That is the common reaction of CEOs, board members and other executives upon learning their business is involved in a mass fatality event. After all they had safety departments, security and insurance. These are successful 99 per cent of the time in preventing events or limiting the damage to property or processes. After all, really bad things only happen to others. It is not a question of if, such as: "If a catastrophic event, an event resulting in a large number of deaths and injuries will occur". It is a question of when. It is a question of where. It is a question of whom.

Businesses have continuity plans. These plans often detail what has to be done; some even detail how things are done. However, few address how to manage the humanitarian aspects of consequence management. It is managing that one percent of events that cause the most damage, trauma and lasting impact on corporations and individuals.

The world has several mass fatality events each year; almost every one of them involves private businesses, who are utterly unprepared for their role. They feel that such events are so large, that it is the government's responsibility to take care of everything. Governments have systems in place. Nonetheless, they reasonably expect coordination and involvement from the affected businesses.

Governments expect that businesses can receive, and transfer data about missing employees. That business can establish and operate a humanitarian assistance centre. A centre where government teams and your own human resource assistance teams operate to assist the families during the recovery phase.

Families and employees also have expectations. They expect that you will be able to answer their questions, facilitate government support, and arrange for the dignified return of their deceased loved ones and personal belongings. Beyond the practical matters, families expect that the company involved will help them adjust to the new normality. This is hard enough for a single loss. It is much more difficult for multiple losses and nearly impossible without experience-driven plans.

This is a board and leadership responsibility. The public know and expect that despite the best technologies, efforts and intentions tragic events will occur. Because of that they expect that businesses are prepared and resourced to effectively, compassionate and professionally manage such events. Can you?